Patent Application of

Justin Page

For

TITLE: NETWORK AND DATABASE SYSTEM FOR PERSONAL PRIVACY PROTECTION

CROSS-REFERENCE TO RELATED APPLICATIONS

Patent No.	Inventor
5,274,547	Zoffel et al.
5,323,315	Highbloom
5,696,965	Dedrick
5,742,775	King
5,752,242	Havens
5,809,478	Greco et al.
5,872,921	Zahariev et al.
5,878,403	DeFrancesco et al
5,943,666	Kleewein et al.
5,999,907	Donner
6.023,694	Kouchi et al.
6,029,149	Dykstra et al.

Foreign Patent Number	Country & Date
97/14108	World Organization,04/97
10-257177	Japan, 09/1998

BACKGROUND OF THE INVENTION

FIELD OF INVENTION

The invention (1,4,9) generally relates to the field of protection of personal data and digital information which is publicly available, and more specifically, to the field of culling electronic and/or digital information and data sources (7) which tend to disclose legally or illegally obtained personal information (while building a database thereof, and monitoring those for changes, additions and deletions, and new entries(5)) and upon the bona fide violation of privacy and at the user's behest, all legal automated means are taken to have the data removed on the individual's behalf. Failing success of the efforts described hereinbefore, the system has a document generation and professional referral component (4), which will expedite the processing of non-automated actions or proceedings.

DESCRIPTION OF PRIOR ART

The transition from an industrial to a computer-based society is rapidly taking place. In this process, the threat to individual privacy has become undeniable, and is well documented. Despite the increasing frequency of "identity theft," and of credit fraud and error, there is no practical and simple way for individuals to protect themselves – either proactively or, where an individual has already been victimized, reactively.

Automated electronic business methods have been the subject of earlier patents. Highbloom discloses a system for periodic monitoring of collateralized property, to determine if individual items of property are being utilized to collateralize multiple loans with different lenders. The system reports to lenders when that occurs. The patent to Donner involves an audit system that searches intellectual property databases, makes comparisons and outputs a report.

The patent to Zoffel et al. involves a system for generating and transmitting credit reports. The patent to Dykstra et al. involves a system which outputs credit reports via facsimile. Kouchi describes a generic system for periodic data retrieval from heterogeneous databases (its heterogeneity pertaining to technical infrastructure and design, but not content or ownership) with subsequent report generation. The rest of the above-listed patents were selected to further illustrate patents in the field of automated electronic methods of credit bureaus and other sources.

SUMMARY

Is is, therefore, the object of the present invention (1,4,9) to protect individual privacy by means of an electronic method which tracks, subscribes, persistently culls databases (which are stored in a database itself) and in the event of any new information found, notifies users electronically of any such information (or not, if they so choose), and alternatively allows them to respond to such information electronically. Failing success of said electronic methods, or where no electronic methods exist, the system generates prepared documents for investigative, administrative and/or legal follow-up (4).

BRIEF DESCRIPTION OF THE DRAWING

Figure 1 is a detailed block diagram of the structure of the network and database system for personal privacy protection.

COMPONENT DESCRIPTIONS

1. A computer program and business method, programmed in Java™ (or any open systems language) which constantly culls various privacy-related databases on behalf of its users, and dispatches new information to the user, will aid the user in the disputation of false information, will reactively alert the user's financial institutions after a theft or security breach, attempt to lessen the user's liability and/or burden by expedited automated methods (where available), and failing electronic resolution, the invention generate the appropriate documents and assign to attorney, private detective or credit specialist for further investigation. The system is dependent upon

2. A secured Internet connection, including routers and hardware and software "firewalls" to prevent unauthorized access.

3. Omitted

4. Legal and Administrative Document Generation System

5. Database of Customer Information and Accounts

6. Omitted

7. A compilation of dynamic information providers and/or privacy offenders,

8. The Internet or a Private or Semi-Private Network

9. Manual and automated e-mail process to continue removal of personal information.

OBJECTS OF THE INVENTION

1. to provide an inclusive means for the protection and restoration of individual consumer privacy;

2. to inform individuals automatically when potential or actual risk or theft exists, and offer to provide further services, if the user so desire and/or requires.

3. to build and maintain a persistently updated database of publicly accessible databases and information, including but not limited to Internet web pages, Internet "newsgroups", the Internet 'WHOIS' database (a database of all Internet domain name registrations), publicly and semi-publicly available information (including government databases), credit bureau databases and law enforcement systems;

4. to create electronic referrals to attorneys, private detectives, security specialists and law enforcement agencies when required;

5. to generate documents relative to the aforesaid referrals in order to expedite the processing of any such action or complaint in the event of an adverse event;

6. to provide constant electronic notice to users of said system and processes of any new information circulating within the aforesaid databases;

7. to reduce the burden on those who have been victimized by identity theft, credit card fraud, Internet domain name theft or other privacy-related offenses;

8. to expedite recuperative or restorative procedures by electronic means or by automatically generating documents based upon the data collected in from the user.

PREFERED EMBODIMENT OF THE INVENTION

The current invention uses distributed and open-system architecture to create easy extensibility. Sources of data are as varied as the methods that could be employed to access them. It is implemented as a platform-portable, language-independent distributed object framework. For example, the present invention could easily act as a back-end resource to existing online providers. The distributed approach allows the system to be accessible through a number of interfaces, for example web browsers, web devices, traditional and interactive television, personal data assistants or on diverse operating systems, such as Sun Solaris™ or Microsoft Windows NT™.

Referring to Figure 1, a diagrammatic representation of access to the Invention's network is shown. Preferably, users access the invention via the Internet, its successors or replacements. The invention shall be accessible to any site with TCP/IP name resolution (although full usage may require further usage of industry digital encryption standards.) The invention is designed with the expansibility of the Internet's infrastructure in mind.

As shown in figure 1, electronic transmissions destined for the invention are routed (1) to a web server (with associated database and "middleware") subsystems) for processing (5). Security is obviously a significant issue for privacy protection systems. Therefore, at the demarcation zone (2) a state-of-the-art hardware and software sub-system to provide unauthorized access, denial of service attacks or other service interruptions.

Data requests could be serviced in a number of ways. For example, data may be accessed using an Oracle Database running on Sun Solaris or on a Microsoft Windows NT Server running on Windows NT.

Although the present invention can be based upon the Internet Protocol (IP), clients are completely isolated from back-end sourcing concerns and do not need to know the IP addresses of object servers. Using this approach, servers may be added simply by connection to the Internet. Consequently, clients are not affected by database, network, operating system, installing system and server software or architectural change. The distributed nature of the system means that it is composed of relatively simple applications that implement a single interface or a small group of interfaces.

The Object Request Broker (ORB) is an "information bus" that connects users to the objects they need to be automatically notified of new information about them, and what (if any) action should be taken.

The present invention uses the latest possible Internet Protocol security devices and digital signatures. This is to ensure system security and the security of the user data.

ABSTRACT

The invention relates generally to the field of protection of personal data and digital information which is publicly available on the Internet or via other means, and more specifically, to the field of persistent culling of electronic and/or digital information and data sources which tend to disclose legally or illegally obtained personal information (while building a database thereof, and monitoring those for changes, additions and deletions, and new entries) and upon a confirmed alleged violation of privacy at the user's behest, all legal automated means are taken to have the data removed on the individual's behalf. Failing success of the efforts described hereinbefore, the system has a document generation and professional referral component (4), which will expedite the processing of non-automated actions or proceedings.